UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/685,726	10/15/2003	Craig H. Rowland	062891.1166	5392

5073 7590 05/30/2007

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2131	

NOTIFICATION DATE	DELIVERY MODE
05/30/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mike.furr@bakerbotts.com
ptomail1@bakerbotts.com

Office Action Summary	Application No.	Applicant(s)	
	10/685,726	ROWLAND, CRAIG H.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *see attachment*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the arguments filed on 28 March 2007.

2. Claims 1-21 are pending in the application.

3. Claims 1-21 have been rejected.

Information Disclosure Statement

4. The examiner has considered the information disclosure statement filed on 28 March 2007.

Response to Arguments

5. Applicant's arguments filed 28 March 2007 have been fully considered but they are not persuasive.

On page 8, the applicant argues that McClure does not teach or suggest, "receiving, from an intrusion detection sensor, one or more packets associated with an alarm indicative of a potential attack on a target host".

The examiner respectfully disagrees. McClure discloses sometimes, in order to "force" a response from the target computer, an intruder may send a malformed packet to a target port. While this known technique increases the likelihood that an open UDP port on the target computer can be identified, this technique also substantially increases the likelihood that the malformed packet could damage the target computer. Also, firewalls or routers may detect and filter out malformed packets, and such packets can alert the target network of an attempted security breach.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-21 are rejected under 35 U.S.C. 102(e) as being anticipated by McClure et al U.S. 7,152,105 B2.

As to claim 1, McClure et al discloses a computerized method for reducing the false alarm rate of network intrusion detection systems, comprising:

receiving, from a network intrusion detection sensor, one or more data packets associated with an alarm indicative of a potential attack on a target host [column 17 line 29 to column 18 line 50];

identifying characteristics of the alarm from the data packets, including at least an attack type and an operating system fingerprint of the target host [column 17 line 29 to column 18 line 50];

identifying the operating system type from the operating system fingerprint [column 17 line 29 to column 18 line 50];

comparing the attack type to the operating system type [column 17 line 29 to column 18 line 50]; and

indicating whether the target host is vulnerable to the attack based on the comparison [column 17 line 29 to column 18 line 50].

As to claims 2 and 17, McClure et al discloses storing the operating system fingerprint of the target host in a storage location for a time period [column 18, lines 20-42].

As to claims 3, 9 and 18, McClure et al discloses the computerized further comprising:

monitoring a dynamic configuration protocol server [column 22, lines 32-67];

detecting that a lease issue has occurred for a new target host [column 22, lines 32-67];

accessing a storage location [column 22, lines 32-67];

determining whether an operating system fingerprint for the new target host already exists in the storage location [column 22, lines 32-67]; and

if the operating system fingerprint for the new target host does exist, then purging the existing operating system fingerprint for the new target host from the storage location [column 22, lines 32-67].

As to claims 4, 10 and 19, McClure et al discloses the computerized further comprising:

monitoring a dynamic configuration protocol server [column 22, lines 32-67];

detecting that a lease expire has occurred for an existing target host [column 22, lines 32-67];

accessing a storage location [column 22, lines 32-67];

determining whether an operating system fingerprint for the existing target host already exists in the storage location [column 22, lines 32-67]; and

if the operating system fingerprint for the existing target host does not exist, then disregarding the lease expire [column 22, lines 32-67]; and

if the operating system fingerprint for the existing target host does exist, then purging the existing operating system fingerprint for the existing target host from the storage location [column 22, lines 32-67].

As to claims 5 and 20, McClure et al discloses the computerized further comprising:

after receiving the data packets, determining whether a format for the alarm is valid [column 23, lines 26-52]; and

if the format is not valid, then disregarding the alarm [column 23, lines 26-52]; otherwise

if the format is valid, then continuing the computerized method with the identifying characteristics step [column 23, lines 26-52].

As to claims 6, 11 and 21, McClure et al discloses automatically alerting a network administrator if the target host is vulnerable to the attack [column 17 line 29 to column 18 line 50].

As to claim 7, McClure et al discloses a system for reducing the false alarm rate of network intrusion detection systems, comprising:

a network intrusion detection system operable to transmit one or more data packets associated with an alarm indicative of a potential attack on a target host [column 17 line 29 to column 18 line 50];

a software program embodied in a computer readable medium, the software program, when executed by a processor, operable to:

receive the one or more data packets [column 17 line 29 to column 18 line 50];

identify characteristics of the alarm from the data packets, including at least an attack type and an operating system fingerprint of the target host [column 17 line 29 to column 18 line 50];

identify the operating system type from the operating system fingerprint [column 17 line 29 to column 18 line 50];

compare the attack type to the operating system type [column 17 line 29 to column 18 line 50]; and

indicate whether the target host is vulnerable to the attack based on the comparison [column 17 line 29 to column 18 line 50].

As to claim 8, McClure et al discloses a storage location operable to store the operating system fingerprint of the target host for a time period [column 26, lines 25-35].

As to claim 12, McClure et al discloses that the software program has no knowledge of the protected network architecture [column 24, lines 50-67].

As to claim 13, McClure et al discloses that the software program has no access to the protected network [column 24, lines 50-67].

As to claim 14, McClure et al discloses that the NIDS is vendor independent [column 12, lines 30-49].

As to claim 15, McClure et al discloses that the NIDS does not support passive operating system fingerprinting [column 12, lines 30-49].

As to claim 16, McClure et al discloses a system for reducing the false alarm rate of network intrusion detection systems, comprising:

means for receiving, from a network intrusion detection sensor, one or more data packets associated with an alarm indicative of a potential attack on a target host [column 17 line 29 to column 18 line 50];

means for identifying characteristics of the alarm from the data packets, including at least an attack type and an operating system fingerprint of the target host [column 17 line 29 to column 18 line 50];

means for identifying the operating system type from the operating system fingerprint [column 17 line 29 to column 18 line 50];

means for comparing the attack type to the operating system type [column 17 line 29 to column 18 line 50]; and

means for indicating whether the target host is vulnerable to the attack based on the comparison [column 17 line 29 to column 18 line 50].

As to claim 20, McClure et al discloses the system further comprising:

after receiving the data packets, means for determining whether a format for the alarm is valid [column 23, lines 26-52]; and

if the format is not valid, then means for disregarding the alarm [column 23, lines 26-52].

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy AM
May 22, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100